Issues in Software System Safety:
Polly Ann Smith, Co.
v.
Ned I. Ludd

C. Michael Holloway

Presented at the 2nd Meeting of the
U.S. Software System Safety Working Group
M.I.T.
February 19-20, 2002

Disclaimers

- This is a work of fiction, although I will pretend it is real
  - The case is not real
  - The accident giving rise to the case is not real
  - The people are not real (with a few obvious exceptions)
  - The software assurance method mentioned is not real
  - The cited precedence cases and federal rules *are real*
- I am not a lawyer, nor do I play one on TV
  - This is not expert legal commentary
  - Several simplifications have been made
- My goal is to stimulate friendly discussion about a few issues over which discussion is often not so friendly

Outline

- Description of the case
  - Facts
  - Initial Litigation
  - Ruling by District Court
  - Ruling by Circuit Court
  - Ruling by Grand Court
- Group discussion of the issues raised by the case
  - What is known about software system safety?
  - What qualifies one as an expert?
  - What is the relationship between safety and other attributes?
  - Others?

The Facts of the Case

- Ludd was injured in crash of a small aircraft he was piloting
  - Low-visibility landing attempt using automated landing system named Amelia, which was built by the Polly Ann Smith, Company
  - Crashed short of the runway
  - Ludd survived the crash, but sustained serious injuries, which left him partially disabled
- Investigation uncovered erroneous software in Amelia
  - Under certain meteorological and geographic conditions, Amelia sent wrong commands to control surfaces
  - Unless overridden by pilot, these commands would cause aircraft to contact the ground several hundred feet short of the runway threshold

Litigation Begins

- Ludd sued Polly Ann Smith, Co.
  - Alleging negligence in design and implementation of Amelia
  - For failing to apply state-of-the-practice software safety techniques to the design and assessment of the system
- Case rested primarily on depositions of G. Clarke, an internationally-recognized software safety researcher,who was prepared to testify that
  - Certain software safety principles represent the current state-of-the-practice
  - Smith's knowledge of these principles was deficient
  - Records showed no application of these principles in the creation and deployment of the Amelia software

Smith Responds

- Polly Ann Smith, Co. did not contest that Amelia software contributed to Ludd's accident, but denied negligence
- Moved to exclude Clarke's proffered testimony because
  - (1) he didn't qualify as an expert witness, or
  - (2) his opinions on the deficiencies in Amelia development did not rise above 'subjective belief or unsupported speculation'*
- Further moved for summary judgment in its favor on the grounds that without Clarke's testimony Ludd did not have any evidence to support his claim of negligence

* *General Electric, Co. v. Joiner*, 522 U.S. 136 (1997)

Smith's Basis for Motions

- On its behalf, Smith offered depositions from its own expert, C. Vantile, an internationally-recognized software researcher, and developer of widely-used techniques for analyzing the correctness of software systems
- Vantile planned to testify that
  - Software safety principles did not represent the state-of-the-practice
  - The true state-of-the-practice was represented by the application of his own techniques for software assurance
  - Smith had applied these techniques in developing Amelia
  - No one could have been expected to discover the flaws in Amelia that led to Ludd's accident

The District Court Rules

- Granted Smith's motion to exclude Clarke's testimony and entered summary judgment for Smith
- Based its ruling on
  - Court's obligation to ensure that proposed expert testimony is both relevant and reliable
  - Clarke's testimony failed the appropriate tests for reliability of the underlying methods upon which it was based, and thus must be excluded
  - Without Clarke's testimony, Ludd had no evidence of negligence by Smith
- Ludd appealed

The Circuit Court Overturns

- Circuit Court asserted that the District Court had abused its discretion in excluding Clarke's testimony
  - Clarke's credentials as an expert were impeccable
    - International reputation
    - Numerous published papers
    - Consultant to companies and government agencies
  - Disallowing such a person's testimony was, on its face, abuse of discretion
- Smith appealed, and the Grand Court agreed to hear the case

The Grand Court Rules

- By a 6-3 decision, the Grand Court
  - Affirmed that the District Court erred in excluding Clarke's testimony
  - Said the Circuit Court's rationale for its judgment was wrong
- Opinion of the court
  - Reaffirmed principle of distinguishing between qualification as an expert and allowing particular testimony
  - Distinguished between 'gatekeeper' and 'arbiter' roles
- Dissenting opinion
  - Agreed with majority's distinctions in principle, but dissented from the application of these distinctions in this case
  - Asserted that neither Clarke's nor Vantile's testimony should have been allowed

Opinion of the Court

- General Observations
  - "Abuse of discretion is the appropriate standard of review."
  - "Federal Rule of Evidence 702 is controlling in this case: 'If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case'."

Opinion of the Court (continued)

- Expert witnesses in this case
  - "Without question, 'scientific, technical, or other specialized knowledge' is necessary 'to understand the evidence' in this case. Thus, the use of expert witnesses is warranted."
  - "Also without question, Ludd's proffered expert witness, G. Clarke, 'qualified as an expert by knowledge, skill, experience, training, or education'. So, too, did C. Vantile, Smith's proffered expert."
  - "Had the District Court failed to qualify either person as an expert, it would have abused its discretion. But the Court did not exclude them as experts; instead, it excluded Clarke's specific testimony as being neither 'based upon sufficient facts or data', nor 'the product of reliable principles and methods.' We must determine whether *that* exclusion was an abuse of discretion."

Opinion of the Court (continued)

- Excluding Clarke's testimony was abuse of discretion
  - "A trial court has wide discretion in determining how to test the reliability of the principles and methods upon which testimony is based; however, this 'is not discretion to perform the function inadequately. Rather, it is discretion to choose among *reasonable* means of excluding expertise that is *fausse* and science that is junky.'*"
  - "The means chosen by the District Court was unreasonable. The Court became, in essence and in fact, the arbiter between conflicting theories, when the evidence does not clearly and convincingly demand, either in our minds or in the minds of many software professionals, that one side be declared wrong and the other right."

* *Kumho Tire Col., Ltd., et al. v. Carmichael et al.*, 526 U.S. 137 (1999), J. Scalia, concurring

Dissenting Opinion

- "We agree with much of what the majority has to say. Certainly, abuse of discretion is the right standard of review. *If* we agreed that Rule 702 applied in this case, we *might* even concur with the analysis presented by our distinguished colleagues. But Rule 702 does not apply."
- "For Rule 702 to apply, there must exist 'scientific, technical, or other specialized knowledge' relevant to the case. There is none here."
- "Although a substantial body of literature exists about every aspect of software engineering, little, if any, of it can rightly be called 'knowledge', especially when safety-critical systems are involved."

Dissenting Opinion (continued)

- "Some basic agreement exists about very general propositions (for example, 'Requirements engineering is difficult.'), but virtually no universal agreement exists about specifics, especially in regard to solutions to problems."
- "An analogy of Newton's third law applies to the field: For every software researcher, there is an equal and opposite software researcher. Opinions abound, but solid evidence (based on either experimentation or rational argument) to support these opinions is rare."
- "In this field, one can almost say that all expertise is *fausse* and all science is junky."

Dissenting Opinion (continued)

- "For these reasons, we do not believe that the proffered testimony on behalf of either Ludd or Smith rises above 'subjective belief or unsupported speculation.'"
- "Thus, the District Court did not abuse its discretion when it disallowed Clarke's testimony."
- "The issue of whether to allow Vantile's testimony was mute when the District Court ruled that, with Clarke's testimony excluded, Ludd did not have a case. Had the issue not been mute, Vantile's testimony should also have been excluded."
- "Perhaps one day there will exist reasonable 'knowledge' in software engineering, but that day is not today."

Paraphrase of Opinions

- Majority
  - Both Clarke and Vantile possess ‘scientific, technical, or other specialized knowledge’ relevant to the case
  - In disallowing Clarke’s testimony, the District Court improperly assumed the role of arbiter of a professional dispute in which both sides have reasonable evidence for their positions
- Dissent
  - Current state of software engineering is such that little worthy of the name ‘specialized knowledge’ exists
  - All Clark and Vantile have to offer is ‘subjective belief or unsupported speculation’
  - Neither qualifies as an expert witness, because neither has reasonable evidence for his position

Time to Vote

- Before we begin discussion, we'll take a vote.
- From the following propositions, choose the one that most closely represents your opinion about this case:
  - I **completely agree** with the **majority** opinion
  - I **completely agree** with the **dissenting** opinion
  - I agree **more** with the **majority** than the dissent
  - I agree **more** with the **dissent** than with the majority
  - I **completely disagree with both** of them
- Does anyone have any clarifying questions to ask before voting?

Let the Discussion Begin!